Claims 1-26 stand rejected under 35 U.S.C. §112, 2nd paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants claim as the invention. Claims 1, 9, 14, and 21 have been indicated as being vague and indefinite. Applicants have suitably amended the claims to overcome this rejection. Claims 2-8, 10-13, 15-20 and 22-26 are similarly rejected for inheriting these deficiencies. These claims are also believed to overcome this rejection in view of the above amendments.

Claim 26 has also suitably been amended consistent with the Office Action's comments.

Claims 1, 3, 6, 7, 9, 10, 14, 16, 17, 20, 21, 23 and 26 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,457,746 (Dolphin). The Dolphin reference is directed to a system and method for access control for portable data storage media to facilitate, for example, secure periodic distribution of several different sets of information through the use of an access code. These decryption access codes are provided to users to allow users to gain access to distributed media. The Dolphin reference teaches one symmetric key for all users wherein different date ranges are associated with the same key depending upon the user. One encryption key is generated from a previous key. The Dolphin references teaches that the access code or key may have expired for one user but the same key is still good for other users. Moreover, the key expiration date apparently used in the Dolphin reference relates apparently only to a public key, and does not relate at all to decryption or private keys. Since only one key is used for all users, Dolphin does not provide the security required for a public key infrastructure system as claimed by applicants.

As to claims 1, 3, 6, 7, 9, 10, 14, 16, 17, 20, 21 and 23 and 26, applicants claim, inter alia, selectable digital signature expiry data including at least both public verification key expiry data and selectable private signing key expiry data. Such a method for providing updated digital signature key pairs in a public key system is not

4

taught or suggested by Dolphin. The Dolphin reference appears to be silent as to providing updated digital signature key pairs. In addition, applicants claim, inter alia, that the digital signature key pairs are not shared among users. Again, Dolphin appears to be silent as to such a system and method for providing selectable digital signature expiry data for public verification expiry data and private signing key expiry data wherein the digital signature key pairs are not shared among users. Claims 3, 6, and 7 also provide novel aspects relating to digital signature key pair updates such as variable update privilege control on a per client, and other novel limitations.

In addition, applicants claimed method and apparatus provides, through a multi client manager, public encryption key expiry data associated with a public encryption key that is selectable on a per client basis. And also generating a new encryption key pair that is not computable from a previous encryption key and associating stored selected expiry data with the new encryption key pair to effect transition from an old encryption key pair to a new encryption key pair. Such a public key based system in not taught or suggested by Dolphin. In contrast, Dolphin teaches computing one code from another code. This type of operation is contrary to the goals of the applicants' invention which is a public key system designed to provide unique encryption and decryption capabilities for each user and wherein the key pairs are not computable from a previous encryption key to ensure protection of encryption encrypted data over time. The selectable expiry data for a public decryption key selectable on a per client basis and generating a new encryption key pair is not computable from the previous encryption keys nor is this taught or suggested by the reference.

Claims 2, 4, 8, 11-13, 15, 18, 22 and 24 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the Dolphin reference in view of U.S. Patent No. 5,901,227 (Perlman). Perlman has been cited as teaching a certification authority using digital certificates that receives keys after they have been generated and attaches a certificate of authenticity to the key and gives it to a user. The office action argues that it would therefore have been obvious to associate digital certificates with time limited keys. However, applicants respectfully note that the claims are directed to, inter alia, selectable

expiry data including both public verification key expiry data, selectable private signing key expiry data, public encryption key expiry data as well as digital signature certificate life time data for variably setting a lifetime end date for a digital signature certificate. Such a system is not disclosed or suggested by the references. As noted above, the Dolphin reference describes a symmetric encryption process. The validity periods of Dolphin are for a symmetric decryption key which is the same for many users. Applicants claim a radically different system, namely, a public key system in which the keys are different for all users. Moreover, Dolphin does not teach or suggest the validity period control of public keys nor the updating of public keys. Dolphin appears to teach using public key pairs to digitally sign secure information for access. It does not teach, for example, the use of public keys for encryption. In fact, if public encryption/private decryption keys were used in Dolphin, one could not compute one key from another as required by the Dolphin reference. Accordingly, combining Dolphin with Perlman is an improper combination, since Dolphin does not teach or suggest public key encryption transitions from an old encryption key pair to a new encryption key pair or digital signature key pairs wherein the digital signature key pairs are not shared among users. It is respectfully noted that, even if the references were properly combinable, for argument's sake, the desired Dolphin system would be inoperable since the encryption keys could not be computed from one another as required, for example, in Col. 13.

Claims 5, 19 and 25 stand rejected under 35 U.S.C. §103 as being unpatentable over the Dolphin reference in view of Applicants' admitted prior art. Again, Dolphin is directed to a symmetric encryption key system that uses one key to generate another key and uses a defined validity period for one key that can be used by many users. Applicants claim a different system as previously described and also claim, inter alia, determining digital signature private key lifetime end dates and digital signature certificate creation time and initiating key pair update requests based on differences between current dates and digital signature private key lifetime end dates is less than an absolute predetermined period of time. Such a mechanism is not taught or suggested by applicants' admitted prior art and there is no discussion of digital signature private key lifetime end dates and digital signature certificate creation dates for a public key system

by Dolphin. Accordingly, applicants respectfully submit that the references are not properly combinable.

For argument's sake, even if the teachings were combinable, such systems use prefixed default settings for all clients. Applicants' claimed invention allows the selection on a per user basis of the digital signature public verification key expiry data and selectable private signing key expiry data which is not taught or suggested by Dolphin or Applicants admitted prior art.

For the reasons stated above, the applicants believes that claims are in condition for allowance and respectfully request that they be allowed. The Examiner is invited to contact the undersigned attorney by telephone or facsimile if the Examiner believes that such a communication would advance the prosecution of the present patent application.

Respectfully Submitted,

By: _C. J. Reckamp_

Christopher J. Reckamp
Registration No. 34,414
Attorney for Applicants

Markison & Reckamp, P.C.
175 W. Jackson Boulevard
Suite 1015
Chicago, Illinois 60604
Telephone: (312) 939-9800
Facsimile: (312) 939-9828